(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
15. August 2002 (15.08.2002)

PCT

(10) Internationale Veröffentlichungsnummer
WO 02/063824 A1

(51) Internationale Patentklassifikation[7]: H04L 9/32

(21) Internationales Aktenzeichen: PCT/DE01/02334

(22) Internationales Anmeldedatum:
28. Juni 2001 (28.06.2001)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
101 05 334.7 5. Februar 2001 (05.02.2001) DE

(71) Anmelder und
(72) Erfinder: **OTTEN, Dieter** [DE/DE]; Nienburger Strasse 4, 49088 Osnabrück (DE).

(74) Anwälte: **SPRINGORUM, Harald** usw.; Kiani & Springorum, Heinrich-Heine-Allee 29, 40213 Düsseldorf (DE).

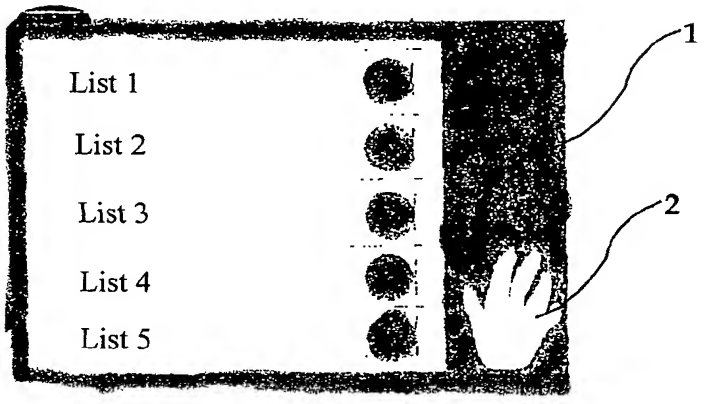
(81) Bestimmungsstaaten *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Bestimmungsstaaten *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ,

[Fortsetzung auf der nächsten Seite]

(54) Title: TELECOMMUNICATIONS PROTOCOL, SYSTEM AND DEVICES FOR ANONYMOUS, VALIDATED ELECTRONIC POLLING

(54) Bezeichnung: TELEKOMMUNIKATIONSPROTOKOLL, -SYSTEM UND -VORRICHTUNGEN ZUR ANONYMEN UND AUTHENTISCHEN ABWICKLUNG EINER ELEKTRONISCHEN WAHL



(57) Abstract: The invention relates to a telecommunications protocol for anonymous, validated electronic polling. According to the invention, a polling point requests an electronic polling card from an electronic polling validator, the electronic polling validator verifies the authorisation of a voter using the electronic polling point to participate in the electronic poll and if said authorisation is verified, sends an electronic polling card to the polling point. The latter then supplies the electronic polling card received from the electronic polling validator with the vote cast by the voter and the electronic polling point forwards the electronic polling card with the vote that has been cast to an electronic polling computer for collection and/or evaluation. The data that has been unequivocally assigned to the voter and the electronic vote that has been cast by the voter are either present throughout all the processing or transmission phases in an encrypted or separate form, or in an encrypted and separate form.

(57) Zusammenfassung: Telekommunikationsprotokoll zur anonymen und authentischen Abwicklung einer elektronischen Wahl, wobei von einer elektronischen Wahlstelle (Pollster) elektronischer Wahlschein von einem elektronischen Wahlleiter (validator) angefordert wird, der elektronische Wahlleiter die Berechtigung eines die elektronische Wahlstelle verwendenden Wählers zur Teilnahme an der elektronischen Wahl prüft und im Falle der Feststellung der Berechtigung des die elektronische Wahlstelle verwendenden Wählers zur Teilnahme an der elektronischen Wahl einen elektronischen Wahlleiter empfangenen elektronischen Wahlschein mmit einer von einem Wähler elektronisch getroffenen Wahl versieht, und die elektronische Wahlstelle den mit der Wahl vesehenen elektronischen Wahlschein an einen elektronischen Wahlrechner (Psephor) zur Sammlung und/oder Auswertung sendet, wobei die der Person des Wählers eindeutig zugeordneten Daten und die von dem Wähler getroffene elektronische Wahl in allen Phasen der Verarbeitung oder Übertragung entweder voneinander getrennt oder verschlüsselt oder voneinander getrennt und verschlüsselt vorliegen.

WO 02/063824 A1

TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Veröffentlicht:

— *mit internationalem Recherchenbericht*

Titel: Telekommunikationsprotokoll, -system und -vorrichtungen zur anonymen und authentischen Abwicklung einer elektronischen Wahl

Die vorliegende Erfindung betrifft ein Telekommunikationsprotokoll, Telekommunikationssystem und Telekommunikationsvorrichtungen zur anonymen und authentischen Abwicklung einer elektronischen Wahl.

Die hier vorgestellte Erfindung dient der Wahl auf elektronischem Wege über Datenverkehrsnetze, wobei Stimmabgabe, Stimmauszählung und die Authentifizierung der zur Wahl zugelassenen Personen durch elektronische Rechner vorgenommen werden.

Eine „klassische" Wahl, also die Wahl ohne intensive elektronische Unterstützung, verläuft, grob gegliedert in 3 Schritten.

1. Die Identifikation und Authentifizierung des Wählers. Der Wähler betritt mit seinem Wahlschein das Wahllokal und identifiziert sich dort, etwa durch Ausweisen mit seinem Personalausweis. Seine Wahlberechtigung weist er durch ein ihm übersandtes Dokument (Authentifizierungsdokument) nach. Der Wahlleiter prüft die Dokumente, überreicht den Wahlschein und kennzeichnet den Wähler in einer Liste. Weiterhin behält er die dem jeweiligen Wähler zugesandten Wahlunterlagen (Authentifizierungsdokumente), so dass die Wahl nur einmal durchgeführt werden kann.

2. Die Stimmabgabe. Der so identifizierte und authentifizierte Wähler wird nun zur Wahl zugelassen. Der Wähler führt in einem abgeschirmten Raum seine Wahl

durch, so daß nur er alleine seine Wahl kennt und übergibt danach seinen Wahlzettel der Wahlurne.

3. Die Stimmauszählung. Die Wahlurne wird unter Aufsicht geöffnet und die Stimmen werden ausgezählt. Es werden die ausgezählten Stimmen aller Wahlurnen zusammengezählt und die Wahl wird anhand dieses Ergebnisses ausgewertet.

Durch dieses Vorgehen wird die Zuordnung einer abgegebenen Wahlstimme zu einem bestimmten Wähler, nämlich dem, der diese Wahlstimme auch abgegeben hat, nahezu ausgeschlossen und die Manipulation der Wahl selbst, als auch die Manipulation des Wahlergebnisses durch mehrmalige Stimmabgabe im Rahmen demokratischer Verfahrensweisen ausgeschlossen. Dieses aufwendige, aber bei jedem Wähler sich wiederholende Verfahren, legt den Einsatz von elektronischen Datenverarbeitungsanlagen nahe. Bekannt sind hier, bei Wahlen mit streng offiziellen Charakter, die üblichen Hilfsmittel, etwa Rechner, Scanner und graphische Aufbereitungssysteme, die allerdings nur bei dem letzten der drei Schritte, der endgültigen Stimmauszählung verwendet werden. Bei Wahlen mit weniger offiziellem Charakter, etwa Umfragen und Abstimmungen, sind schon elektronische Verfahren im Einsatz. Die periodisch neu aufgestellte Rangliste populärer Musikstücke durch Wahl des Titels und des Interpreten ist heutzutage im Internet möglich. Hierbei wird allerdings der Datensicherheit zuliebe auf die Authentifizierung des Wählers verzichtet, so dass eine mehrfache Stimmabgabe möglich ist. Auch bei den im Internet durchgeführten Umfragen und Wahlen zu bestimmten Produkten, bei welchen die Angabe von Name und Adresse zum möglichen Gewinn von Preisen führt, ist die strikte Trennung von Wähler und die von ihm durchgeführte Wahl nicht vollzogen, was anhand der hierauf folgenden Flut neuer und nur das gewählte Produkt betreffende Werbung leicht erkannt werden kann.

Grundsätzlich wäre es möglich eine Wahl nach dem Stand der Technik, so wie sie - wie oben beschrieben - auch im Wahllokal abläuft im Rahmen eines durch eine Datenverkehrsnetz verbundenen Systems von Rechner abzuwickeln.

Dies würde zu einem Verfahren führen, bei dem

- von einer elektronischen Wahlstelle ein elektronischer Wahlschein von einem elektronischen Wahlleiter angefordert wird,
- der elektronische Wahlleiter die Berechtigung eines die elektronische Wahlstelle verwendenden Wählers zur Teilnahme an der elektronischen Wahl prüft und im Falle der Feststellung der Berechtigung des die elektronische Wahlstelle verwendenden Wählers zur Teilnahme an der elektronischen Wahl einen elektronischen Wahlschein an die Wahlstelle sendet,
- die elektronische Wahlstelle den vom elektronischen Wahlleiter empfangenen elektronischen Wahlschein mit einer von einem Wähler elektronisch getroffenen Wahl versieht, und
- die elektronische Wahlstelle den mit der Wahl versehenen elektronischen Wahlschein an einen elektronischen Wahlrechner zur Sammlung und/oder Auswertung sendet.

Ein solches aus der Vorgehensweise in einem Wahllokal her bekanntes Verfahren wäre jedoch aus verschiedenen Gründen zur Durchführung einer gewissen Anforderungen genügenden Wahl ungeeignet.

Offizielle Wahlen müssen gewissen gesetzlichen Anforderungen genügen. In der Bundesrepublik Deutschland müssen sie etwa im Falle der Wahl zum Deutschen Bundestag allgemein, unmittelbar, frei, gleich und geheim sein (vgl. Art. 39 Abs. 1 GG der Bundesrepublik Deutschland).

Einige dieser Anforderungen lassen sich nur rechtlich und nicht technisch herstellen, so etwa die Freiheit der Wahl.

Die Allgemeinheit und Unmittelbarkeit der Wahl kann jedoch durch ein elektronisches Wahlverfahren erheblich unterstützt werden, da der für die konventionelle Abhaltung von Wahlen erforderliche organisatorische Aufwand in Gestalt der Bildung vieler kleiner ört-

lich verteilter Wahlvorstände maßgeblich durch elektronische Systeme vor Ort wählernah reduziert werden kann.

Auch muß eine - gewissen Mindestanforderungen genügende - Wahl gleich und geheim sein. Die Gleichheit bedingt, daß jeder Wahlberechtigte nur eine Stimme abgeben darf wohingegen der geheime Charakter darin seinen Ausdruck findet, daß nicht nachvollzogen werden kann, wer wie gewählt hat.

Aus den letzten beiden Forderungen (Gleichheit und Geheimnis der Wahl) ergeben sich jedoch gegenläufige Anforderungen an das zu verwendende Wahlsystem. Zum einen bedingt die Forderung nach der Gleichheit der Wahl, daß eine Identifikation und Authentifizierung des Wählers erfolgt, zum anderen darf jedoch nach dem dieses festgestellt ist die von ihm getroffene Wahl nicht nachvollzogen werden können.

Diese gegenläufigen Forderungen werden im Wahllokal durch das eingangs beschriebene Procedere eingehalten.

Während man nun im Wahllokal aufgrund dessen, daß der dort persönlich anwesende Wahlvorstand das Wahlgeschehen mit den beteiligten Personen stets im Blick hat diesen Anforderungen leicht zu genügen ist, so ist dies auf elektronischem Wege so nicht möglich. Hier unterliegen die zu übertragenden Datagramme während ihrer Übertragung in einem Datenverkehrsnetz potentiellen Angriffen von Außen. Dies wäre insbesondere im Falle öffentlicher Wahlen zu Staatsorganen angesichts der sich hieraus womöglich ergebenden massenweisen Manipulationsmöglichkeiten eine echte Gefahr für eine Demokratie, die sich solcher Verfahren bedienen würde.

Andererseits besteht jedoch auch - gerade aus dem Wunsch nach mehr direkter Demokratie heraus - ein Interesse Wahlen mittels elektronischer Systeme einfacher durchführen zu können und damit mehr Entscheidungen allgemein und unmittelbar treffen zu können.

In diesem Zusammenhang sei angemerkt, daß der Begriff Wahlen im Rahmen dieser Schrift allgemein im Sinne jeglicher Abstimmung, somit auch etwa im Sinne von Bürgerentscheiden oder Volksbegehren oder Ähnlichem gemeint ist.

Die Aufgabe der vorliegenden Erfindung ist es daher ein elektronisches Wahlsystem anzugeben, welches sowohl die Anonymität (also das Geheimnis der Wahl) als auch die Authentizität (mithin auch die Gleichheit der Wahl) gleichermaßen technisch gewährleistet.

Diese Aufgabe wird durch ein elektronisches Telekommunikationsprotokoll zur anonymen und authentischen Abwicklung einer elektronischen Wahl gelöst, wobei von einer elektronischen Wahlstelle ein elektronischer Wahlschein von einem elektronischen Wahlleiter angefordert wird, der elektronische Wahlleiter die Berechtigung eines die elektronische Wahlstelle verwendenden Wählers zur Teilnahme an der elektronischen Wahl prüft und im Falle der Feststellung der Berechtigung des die elektronische Wahlstelle verwendenden Wählers zur Teilnahme an der elektronischen Wahl einen elektronischen Wahlschein an die Wahlstelle sendet, die elektronische Wahlstelle den vom elektronischen Wahlleiter empfangenen elektronischen Wahlschein mit einer von einem Wähler elektronisch getroffenen Wahl versieht, und die elektronische Wahlstelle den mit der Wahl versehenen elektronischen Wahlschein an einen elektronischen Wahlrechner zur Sammlung und/oder Auswertung sendet und welches dadurch gekennzeichnet ist, daß die der Person des Wählers eindeutig zugeordneten Daten und die von dem Wähler getroffene elektronische Wahl in allen Phasen der Verarbeitung oder Übertragung entweder voneinander getrennt oder verschlüsselt oder voneinander getrennt und verschlüsselt vorliegen.

Auch dient der Lösung dieser Aufgabe ein elektronischer Wahlleiter (Validator), vorzugsweise ein Server-Rechner-System, welcher, vorzugsweise über ein Telekommunikationsnetzwerk, mit mindestens einer elektronischen Wahlstelle (Pollster), vorzugsweise einem Client-Rechner-System, verbunden ist, und der elektronische Wahlleiter programmtechnisch so eingerichtet ist, daß er die Berechtigung eines die elektronische Wahlstelle verwendenden Wählers zur Teilnahme an einer elektronischen Wahl prüft, wobei auch er dadurch gekennzeichnet ist, daß die der Person des Wählers eindeutig zugeordneten Daten und die von dem Wähler getroffene elektronische Wahl in allen Phasen der Verarbeitung auf dem elektronischen Wahlleiter oder Übertragung zum oder vom elektronischen Wahlleiter entweder voneinander getrennt oder verschlüsselt oder voneinander getrennt und verschlüsselt vorliegen.

Auch ein elektronischer Wahlrechner (Psephor, Urne), vorzugsweise ein Server-Rechner-System, welcher, vorzugsweise über ein Telekommunikationsnetzwerk, mit mindestens einer elektronischen Wahlstelle (Pollster), vorzugsweise einem Client-Rechner-System, verbunden ist, wobei der elektronische Wahlrechner programmtechnisch so eingerichtet ist, daß er eine Sammlung und/oder Auswertung der, an ihn von der elektronischen Wahlstelle gesendeten elektronischen Wahlscheine vornimmt und der ebenfalls dadurch gekennzeichnet ist, daß die der Person des Wählers eindeutig zugeordneten Daten und eine vom Wähler getroffene elektronische Wahl in allen Phasen der Verarbeitung auf dem elektronischen Wahlrechner oder Übertragung zum oder vom elektronischen Wahlleiter entweder voneinander getrennt oder verschlüsselt oder voneinander getrennt und verschlüsselt vorliegen, dient der Lösung der vorstehenden Aufgabe.

Hiernach enthalten somit Datenpakete (auch Datagramme oder Telegramme genannt) entweder keine Angaben über die Wähleridentität oder sie enthalten Angeben hierzu (nämlich zum Zwecke der Identifizierung und Authentifizierung), dann aber liegen sie verschlüsselt vor, was im Ergebnis zu einer sogenannten informationellen Gewaltenteilung führt und Anonymität und Authentizität der Wahl sichert.

Eine besonders bevorzugte Ausführungsform des Telekommunikationsprotokolls zur anonymen und authentischen Abwicklung einer elektronischen Wahl ist dadurch gekennzeichnet, daß die elektronische Wahlstelle den elektronischen Wahlschein mit der getroffenen Wahl und mit einer dem Wähler zugeordneten Kennung versehen, verschlüsselt an den elektronischen Wahlleiter zurücksendet, der elektronische Wahlleiter den an ihn zurückgesandten verschlüsselten elektronischen Wahlschein signiert und dann wieder von ihm signiert an die elektronische Wahlstelle sendet, die elektronische Wahlstelle den mit der Wahl versehenen und von dem elektronischen Wahlleiter signierten elektronischen Wahlschein wieder entschlüsselt, die dem Wähler zugeordnete Kennung entfernt und den elektronischen Wahlschein im Falle seiner Authentizität ohne die Kennung aber mit Signatur an den elektronischen Wahlrechner zur Sammlung und/oder Auswertung sendet.

Bei der Durchführung der elektronischen Wahl werden vorzugsweise Codierungs- und Verschlüsselungsverfahren angewendet, welche die während der elektronischen Wahl erzeugten Daten, etwa Personaldaten und Wahldaten, so verschlüsseln, daß im Fall eines nicht authorisierten Zugriffes, diese Daten unlesbar und somit auch unbrauchbar sind. Weiterhin können nicht nur diese Codierungs- und Verschlüsselungsverfahren in dem Wahlverfahren verwendet werden, sondern es werden besonders bevorzugterweise auch sogenannte private Codierungs- und Verschlüsselungsverfahren verwendet, welche nur jeweils dem elektronischen Wahlleiter (Validator), dem elektronischen Wahlrechner (Psephor) und der elektronischen Wahlstelle (Pollster) bekannt sind. Diese privaten Codierungs- und Verschlüsselungsverfahren sind also nur dem jeweiligen Rechner, welcher sie anwendet bekannt, d.h. nur er allein kann ein Datenpaket mit diesen Verfahren ver- und danach auch wieder entschlüsseln. Auch Codierungs- und Verschlüsselungsverfahren, welche die Nutzung, also auch das Lesen, von Daten nur bestimmten Gruppen erlauben und andere Gruppen von dieser Nutzung ausschließen, können verwendet werden. Diese Maßnahme, nämlich die Verwendung unterschiedlicher Codierungs- und Verschlüsselungsverfahren, bildet die Grundlage für ein Übergabeverfahren von Datenpaketen, welche nun zwar von dem Empfänger sortiert, gezählt und verwaltet werden können, wobei aber die ursprüngliche Information der Datenpakete dem Empfänger nicht bekannt ist. Hierdurch ist es möglich, daß ein Datenpaket, mit für den derzeitigen Besitzer unbekannten Inhalt, von diesem Besitzer auf seinen Zugang hin signiert werden kann, etwa in Form einer geänderten Statuskennzahl. Dadurch können Verfahrensabläufe formal kontrolliert und nachvollzogen werden, ohne daß die Gefahr der Informationspreisgabe droht. Weiterhin kann auch die Verschlüsselung der Datenpakete unsymmetrisch ausgeführt sein. Hierbei ist der Sender des von ihm verschlüsselten Datenpaketes selbst nicht mehr in der Lage das Datenpaket zu entschlüsseln, dies kann nur ein bestimmter Empfänger. Diese Verschlüsselungsstruktur erhöht die Sicherheit des Datenpaketes hinsichtlich einer möglichen Veränderung während der Übertragung. Ein solchermaßen verschicktes Datenpaket kann etwa folgende Struktur aufweisen:

$$A_{pub}(B_{priv}(\text{nachricht});\text{nachricht})$$

Wobei A hier den Empfänger darstellt und B der Sender sein soll. Dieses Datenpaket enthält zweimal die gleiche Nachricht. Einmal ist diese Nachricht mit einem privaten Code von dem Sender B verschlüsselt, das andere mal liegt sie unverschlüsselt vor. Das gesamte Datenpaket ist nochmals mit dem öffentlichen Schlüssel des Empfängers A_{pub} codiert. Nur dieser kann das Datenpaket öffnen und dann die unverschlüsselte Nachricht lesen. Der Empfänger A kann nicht die mit dem privaten Code des Senders verschlüsselte Nachricht entschlüsseln. Diese dient nur einer möglichen Kontrolle durch den Sender, ob das Datenpaket während der Übertragung verändert wurde. Ist dies der Fall, sind also die beiden anfangs identischen Nachrichten nicht mehr identisch, wurde an der Nachricht unauthorisiert manipuliert. Ein möglicher Manipulator müßte um ein solch strukturiertes Datenpaket unbemerkt verändern zu können an zwei, an getrennten Orten, vorliegende Schlüssel gelangen.

Die eigentliche elektronische Wahl nach dem hier vorliegenden Telekommunikationsprotokoll verläuft vorzugsweise dabei in folgenden 11 Schritten: Alle Datenpakete, die im Rahmen der elektronischen Wahl nach dem hier vorliegenden Telekommunikationsprotokoll transferiert werden, sind zumindest mit einem Verschlüsselungsverfahren codiert. Im ersten Schritt wird der Wahlvorgang eröffnet, hierbei wird eine Wahlanmeldung w des Wählers, bei dem elektronischen Wahlleiter, dem Validator, vorgelegt und auf eine Wahlberechtigung des jeweiligen Wählers hin überprüft. Hierzu wird von der elektronischen Wahlstelle, dem sogenannten Pollster, eine Verbindung zum Validator über das Netzwerk hergestellt. Ein Datenpaket, welches die Wahlanmeldung w enthält wird nun vom Pollster zum Validator übermittelt. Der Validator überprüft hierauf die vom Pollster übermittelte, nämlich die in dem Datenpaket enthaltene digitale Wahlanmeldung w, indem er diese mit den, vorzugsweise in einem TrustCenter hinterlegten, digitalen Daten vergleicht und dann eine Wahlberechtigung für diesen Wähler entweder bestätigt oder den Wahlvorgang bei etwaigen Unstimmigkeiten sofort abbricht. Liegt nun die Wahlberechtigung vor, überprüft der Validator, ob eine Wahlfreigabe erteilt werden kann. Hierzu kontrolliert er das Wählerverzeichnis auf einen möglichen Eintrag. Liegt dort schon ein Stimmzettel des Wählers mit der vorliegenden Wahlberechtigung vor, so wird der Wahlvorgang an dieser Stelle

ebenfalls abgebrochen. Dadurch wird die mehrfache Stimmabgabe unterbunden. Ist noch kein Stimmzettel des Wählers auf diese Wahlberechtigung hin abgegeben worden, so ist die Wahlfreigabe noch zu erteilen. Zur endgültigen Wahlfreigabe muß nun noch die ordnungsgemäße Identifikation des Wählers erfolgen. Die Identifikation des Wählers erfolgt ebenfalls online. Hierzu wird wiederum ein Datenpaket vom Pollster an den Validator geschickt. Dieser vergleicht dann diese in dem Datenpaket übermittelten Daten mit den vorliegenden im Wählerverzeichnis eingetragenen und für diese Wahl gültigen Daten. Liegt nun dort eine Eintragung mit den entsprechenden Daten vor, so hat sich der Wähler ordnungsgemäß identifiziert. Dem ordnungsgemäß identifizierten Wähler steht nun die Möglichkeit der Wahl zu. Der Validator erteilt nun dem Pollster die Wahlfreigabe für diesen ordnungsgemäß identifizierten Wähler. Hierzu wird die Wahlfreigabe in Form eines Datenpaketes von dem Validator zum Pollster transferiert. Ohne die erteilte Wahlfreigabe ist keine weitere Datenübermittlung des Pollsters zu dem Validator zur Weiterführung dieses bereits eingeleiteten Wahlvorgangs mehr möglich.

Nach der erteilten Wahlfreigabe wird ein elektronischer Wahlschein, vorzugsweise ein Datagramm, etwa besonders bevorzugterweise auch in der Form einer Webseite oder auch einer e-mail, an den Pollster und damit an den zur Wahl berechtigten Wähler übermittelt. Nun wird die eigentliche Wahl durchgeführt. Hierzu muß der vom Validator erteilte und zum Pollster übermittelte elektronische Wahlschein ausgefüllt werden, vorzugsweise wird hierzu eine elektronische Zeigevorrichtung, etwa eine Maus oder ein elektronischer Stift verwendet. Dadurch wird der Bedienkomfort erhöht und die Anzahl ungültiger Stimmzettel wird reduziert. Der so erzeugte Wahlstring ws (die ausgefüllte Webseite, also der mit der Wahl versehene elektronische Wahlschein) wird vom Pollster verschlüsselt und zum Validator zurückgesandt. Der Validator ist nun nicht in der Lage diesen elektronischen Wahlschein zu entschlüsseln, da er nicht über die notwendigen Informationen, also den Entschlüsselungscode verfügt. Der Validator signiert den Wahlschein, d.h. er stellt die Wahlscheinabgabe bis zu diesem Schritt und die formale Richtigkeit des elektronischen Wahlscheins sicher. Der so signierte Wahlschein (Stimmzettel) wird danach an den Pollster zurückgeschickt. Der Pollster entschlüsselt den vom Validator signierten elektronischen

Wahlschein, er entfernt die dem Wähler zugeordnete Kennung (etwa alle Personaldaten oder auch eine anonymisierte Kennung) und sendet ein Datenpaket, welches den Wahlstring aufweist, zu dem elektronischen Wahlrechner (der Wahlurne), also dem Psephor. Mit dem Eingang des elektronischen Stimmzettels und seiner Speicherung in der Wahlurne wird das Wählerverzeichnis für den entsprechenden Wähler gesperrt. Hierzu genügt ein einfacher elektronischer Vermerk, etwa eine Änderung der Statusangabe in dem jeweiligen Feld des Wählerverzeichnisses. Somit ist es ausgeschlossen, daß ein Wähler seine Stimme mehrfach abgeben kann, andererseits ist es aber auch beim Abbruch der Wahl durch einen technischen Defekt, etwa einem Stromausfall und der damit bedingten Unterbrechung des Datenflusses in dem Wahlnetzwerk möglich, daß dieser Wähler die Wahl erneut durchführen kann. Nach einer vollständigen ordnungsgemäß durchgeführten Wahl erhält der Wähler eine Meldung, die ihm dies ausdrücklich bestätigt. Der elektronische Wahlleiter sendet sodann an den Wähler der bereits gewählt hat keinen Wahlschein mehr; evtl. bereits mehrfach angeforderte Wahlscheine werden nur in Form des ersten bei dem Psephor eingehenden und ordnungsgemäß signierten Wahlscheines berücksichtigt; alle weiteren werden nicht berücksichtigt. An dem vereinbarten Wahlstichtag nach Schließung der Wahllokale, also auch der Trennung des Pollsters von dem Wahlnetzwerk, werden die verschlüsselten Voten von dem Psephor in elektronische Zwischenspeicher transferiert und danach vollständig dem Validator übergeben, der dann die Auszählung vornimmt und danach das Ergebnis berechnet.

Die Anwendung digitaler Signaturen bietet hierbei die Möglichkeit den Verfahrensablauf sicher und komfortabel zu gestalten. So sind mit digitalen Signaturen versehenen Datenpakete eindeutig dem Validator, Psephor oder Pollster zuzuordnen, je nachdem wer von den oben genannten Wahlnetzteilnehmern das jeweilige Datenpaket signiert hat. Die digitale Signatur übernimmt hierbei auch die Funktion einer eindeutig zu identifizierenden Unterschrift, so daß die signierten Datenpakete garantiert in einer bestimmten Weise überprüft und bearbeitet sind. So signiert der Validator den vom Wähler ausgefüllten und vom Pollster übermittelten Stimmzettel ohne von dessen Inhalt Kenntnis erlangen zu können. Die dann dem Datenpaket zugefügte Signatur des Validators garantiert dem Pollster somit, daß

das zurück transferierte Datenpaket ordnungsgemäß weiter bearbeitet werden und damit an der Wahl teilnehmen kann. Der Wähler sieht in diesem Schritt, daß der Validator seine eigene Wahl angenommen, also signiert hat, er sieht weiterhin, daß es sich um seine eigene von ihm vorgenommene Wahl handelt, da er das signierte und ihm rückübersandte Datagramm im gegensatz zum signierenden Validator entschlüsseln und prüfen kann, ob hieran unauthorisierte Veränderungen vorgenommen wurden.. Somit ist eine Übergabe eines durch den Validator und durch den jeweiligen Wähler geprüften und für korrekt befundenen Wahlscheins an den Psphor gesichert. Auch ist diese Übergabe anonym, da der Pollster die Kennung aus dem Datenpaket vorher entfernt ohne die Signatur zu beschädigen.

So schützt das erfindungsgemäße Telekommunikationsprotokoll in dieser Ausführungsform besonders wirksam vor einer unerwünschten Wahlmanipulation.

Zum Betrieb der vorstehend erläuterten Ausführungsform des erfindungsgemäßen Telekommunikationsprotokolls dienen vorzugsweise

auch ein elektronischer Wahlleiter (Validator) der programmtechnisch so eingerichtet ist, daß er die Berechtigung eines eine elektronische Wahlstelle verwendenden Wählers zur Teilnahme an einer elektronischen Wahl prüft und im Falle der Feststellung der Berechtigung des die elektronische Wahlstelle verwendenden Wählers zur Teilnahme an der elektronischen Wahl einen elektronischen Wahlschein an die Wahlstelle sendet und der elektronische Wahlleiter einen an ihn von der elektronischen Wahlstelle zurückgesandten verschlüsselten elektronischen Wahlschein signiert und dann wieder so von ihm signiert an die elektronische Wahlstelle sendet, sowie

auch ein elektronischer Wahlrechner (Psephor, Urne) der programmtechnisch so eingerichtet ist, daß auf er nur solche elektronischen Wahlscheine sammelt und/oder auswertet, die auch von einem elektronischen Wahlleiter signiert sind.

Eine weitere Ausführungsform des Telekommunikationsprotokolls zur anonymen und authentischen Abwicklung einer elektronischen Wahl ist dadurch gekennzeichnet, daß die dem Wähler zugeordnete Kennung eine den Wähler identifizierende Identifikation ist.

Auch kann die dem Wähler zugeordnete Kennung diesem anonym zugeordnet sein und so keine Identifikation des Wählers darstellen. Vorzugsweise kann dies dadurch geschehen, daß schon in den ersten Schritten der elektronischen Wahl eine Eliminierung der wählerspezifischen Daten, etwa der Personaldaten stattffindet. Je früher eine solche direkte Anonymisierung des Wählers durchgeführt wird, um so sicherer ist der Wähler vor einer Identifikation seiner Person durch Unbefugte.

Eine weitere Ausführungsform des Telekommunikationsprotokolls zur anonymen und authentischen Abwicklung einer elektronischen Wahl ist dadurch gekennzeichnet, daß die elektronische Wahlstelle den mit der Wahl versehenen und von dem elektronischen Wahlleiter signierten elektronischen Wahlschein wieder entschlüsselt, die dem Wähler zugeordnete Kennung entfernt und den elektronischen Wahlschein ohne die Kennung aber mit Signatur an den elektronischen Wahlrechner nur dann zur Sammlung und/oder Auswertung sendet, wenn die elektronische Wahlstelle die Authentizität des signierten elektronischen Wahlscheins derart feststellt, daß die dem Wähler zugeordnete Kennung nach Empfang vom elektronischen Wahlleiter der Kennung entspricht, wie sie von der elektronischen Wahlstelle an den elektronischen Wahlleiter gesendet wurde.

Eine andere Ausführungsform des Telekommunikationsprotokolls zur anonymen und authentischen Abwicklung einer elektronischen Wahl ist dadurch gekennzeichnet, daß die elektronische Wahlstelle den mit der Wahl versehenen und von dem elektronischen Wahlleiter signierten elektronischen Wahlschein wieder entschlüsselt, die dem Wähler zugeordnete Kennung entfernt und den elektronischen Wahlschein ohne die Kennung aber mit Signatur an den elektronischen Wahlrechner nur dann zur Sammlung/Auswertung sendet, wenn die elektronische Wahlstelle die Authentizität des signierten elektronischen Wahlscheins derart feststellt, daß die vom Wähler getroffene Wahl der Wahl entspricht, wie sie von der elektronischen Wahlstelle an den elektronischen Wahlleiter gesendet wurde.

Die vorgenannten Ausführungsformen beziehen sich dabei auf eine besonders sichere Art der Übermittlung eines bereits signierten elektronischen Wahlscheines von der elektroni-

sche Wahlstelle zum elektronischen Wahlrechner, die die Art der Überprüfung des Inhaltes des elektronischen Wahlscheines durch die elektronische Wahlstelle betreffen.

Eine weitere Ausführungsform des erfindungsgemäßen Telekommunikationsprotokolls ist dadurch gekennzeichnet, daß auf dem elektronischen Wahlrechner elektronische Wahlscheine nur gesammelt nicht jedoch ausgewertet werden. Vorzugsweise werden dabei die vom elektronischen Wahlrechner gesammelten elektronischen Wahlscheine an den elektronischen Wahlleiter zur Auswertung gesendet.

Eine besonders bevorzugte Ausführungsform des Telekommunikationsprotokolls zur anonymen und authentischen Abwicklung einer elektronischen Wahl ist im weiteren dadurch gekennzeichnet, daß nur solche elektronischen Wahlscheine ausgewertet werden, die auch vom elektronischen Wahlleiter signiert sind. Diese Ausführungsform ist eine zusätzliche Sicherheitsmaßnahme, welche vorzugsweise am Ende der Wahl, etwa dem Psephor oder auch dem Validator einen weiteren Kontrollschritt ermöglicht.

Eine weitere Ausführungsform des Telekommunikationsprotokolls zur anonymen und authentischen Abwicklung einer elektronischen Wahl ist dadurch gekennzeichnet, daß die Auswertung der elektronischen Wahlscheine in Form einer Zählung, vorzugsweise nach Wahlkategorien, der jeweils getroffenen Wahl also wie bei einer politischen Wahl oder Stimmabgabe i.d.R. üblich erfolgt.

Zum Betrieb des erfindungsgemäßen Telekommunikationsprotokolls kann mindestens eines der folgenden Verschlüsselungsverfahren Verwendung finden:

- ein Blinding-Verfahren, und/oder
- ein RSA-Verschlüsselungsverfahren, und oder
- eine Hashfunktion, vorzugsweise eine Einweg-Hashfunktion.

Bei einem Blinding-Verfahren werden die Daten mit Hilfe einer nur dem Anwender bekannten Zahl so verschlüsselt, daß sie zur formellen Bearbeitung, etwa der Zählung, Archivierung und Kennzeichnung mit einer digitalen Signatur, zur Verfügung stehen, der eigent-

liche Inhalt, etwa der Wahlstring aber nur dem Anwender bekannt ist. Hierbei ist besonders zu beachten, das eine Nachricht, welche geblindet und dann zur Signatur verschickt wurde nach ihrer Rückübertragung zusammen mit der Signatur von dem Ersteller der Blindung entblindet werden kann ohne die Signatur zu zerstören. Es können also Nachrichten oder Datenpakete für den jeweiligen Empfänger unlesbar, da sie geblindet wurden, nur zum Zwecke des Signaturerhaltes verschickt werden. Die so signierten Datenpakete können hiernach auch von ihrem ursprünglichen Ersteller entblindet und dann weiterbearbeitet werden. Die Signatur stellt nur sicher, daß die Datenpakete formal geprüft wurden.

In einer weiteren Ausführungsform werden die Daten über eine Hashfunktion gesichert. Die Sicherung der Daten über eine Hahfunktion oder sogar eine Einweghasfunktion ermöglicht es die Chronologie der Ereignisse des elektronischen Wahlverfahrens so zu verändern, daß sie nicht mehr rekonstruiert werden können und somit eine Rekonstruktion der Wahl auch während des laufenden Wahlvorganges von nicht authorisierten Stellen nicht möglich ist. Hierzu wird dem Datensatz ein für ihn signifikantes Datum zugeteilt, welches aber keinen Aufschluß über dem eigentlichen Datensatz zuläßt. Die Verwendung einer Hashfunktion anstelle der eigentlichen Nachricht kann zudem auch noch zu einer deutlichen Verringerung des Datenpaketgröße führen und damit die Übertragungszeit erheblich verringern.

Die zum Betrieb des erfindungsgemäßen Telekommunikationsverfahrens verwendete elektronische Wahlstelle (Pollster), vorzugsweise ein Client-Rechner-System, ist, vorzugsweise über ein Telekommunikationsnetzwerk, mit einem elektronischen Wahlleiter (Validator), vorzugsweise einem ersten Server-Rechner-System und einem elektronischen Wahlrechner (Psephor, Urne), vorzugsweise einem zweiten Server-Rechner-System, verbunden und dadurch gekennzeichnet, daß sie programmtechnisch so eingerichtet ist, daß sie ihren Kommunikationsverkehr zum elektronischem Wahlleiter und zum elektronischen Wahlrechner nach einer Ausführungsform des erfindungsgemäßen Telekommunikationsprotokolls abwickelt.

Die elektronische Wahlstelle (Pollster) kann dabei eine Lesevorrichtung zum Lesen eines elektronisch lesbaren Datenträgers, vorzugsweise eines nicht wiederbeschreibbaren Datenträgers, besonders bevorzugterweise einer Chipkarte oder einer CD-ROM oder auch einer DVD, aufweisen, die zur Authentifizierung oder Identifikation des Wählers mittels des nicht wiederbeschreibbaren Datenträgers dient.

So kann die Authentifizierung/Identifikation des Wählers mit Hilfe einer elektronisch lesbaren Mediums durchgeführt werden. Diese Automatisierung der Authentifizierung bedeutet eine eindeutige Zeitersparnis und weniger Personal, da nicht jeder Wähler durch Augenschein identifiziert werden muß, sondern sich etwa mit Hilfe seiner Chipwahlkarte ausweist, welche heutzutage fälschungssicher erstellt werden können.

Auch kann die elektronische Wahlstelle (Pollster) eine Lesevorrichtung zur Durchführung einer biometrischen Identifikation, vorzugsweise einen Retina-Scanner oder ein Fingerabdrucklesegerät, besonders bevorzugterweise ein Sensorfeld, aufweisen, die zur Identifikation des Wählers dient. In dieser ganz besonderen Ausführungsform wird die Identifikation des Wählers mit Hilfe einer biometrischen Methode, etwa durch Scannen einer Handfläche, durchgeführt. Auch ist der Sicherheitsaspekt bestimmend, da biometrische Meßmethoden eine eindeutige Identifkation zulassen, so daß diese Identifikationsmethode zusammen mit einer sicheren Authentifikation eine Manipulation der Wahl am Pollster den Wähler betreffend nahezu ausschließen.

Weiterhin kann die elektronische Wahlstelle (Pollster) auch ein elektronisches Stimmabgabe-Panel (1) aufweisen, welches vorzugsweise auch eine Leseeinheit für die elektronisch lesbare Chipkarte aufweist und es so auch unerfahrenen Wählern - bei entsprechender Bedienerführung - ermöglicht, die Wahlstelle ohne fremde Hilfe zu benutzen, was ebenfalls der Gewährleistung der Anonymität dient.

Auch können die zum Betrieb der elektronischen Wahlstelle (des Pollsters) benötigten Software-Module auf nicht wiederbeschreibbarem Datenträger, vorzugsweise auf CD-ROM oder auf DVD vorliegen. Hierdurch wird eine Manipulation - etwa durch Trojaner - des Pollsters erschwert die Mobilität des Pollster aber erhöht, wodurch auch der Heim-PC als

elektronische Wahlstelle in Frage kommt. Auch eine Kombination der CD-ROM als Träger der Betriebssoftware-Module und als Identifikationsausweis des Wählers kommt hierdurch in Frage.

Alle - insbesondere die vorstehend beschriebenen - Ausführungsformen des Telekommunikationsprotokolls nach der vorliegenden Erfindung wie auch die Verfahren zum Betrieb der einzelnen Systemkomponenten nach der vorliegenden Erfindung, also insbesondere von Validator, Pollster und Psephor eignen sich jeweils selbstverständlich als Computerprogrammprodukt, welches ein computerlesbares Medium mit Computerprogramm-Code-Mitteln aufweist oder als ein Computerprogramm auf einem elektronischen Trägersignal und bei dem jeweils nach Laden des Computerprogramms der jeweilige Computer durch das Programm zum Betrieb der hier beschriebenen jeweiligen Ausführungsform des erfindungsgemäßen Telekommunikationsprotokolls oder des erfindungsgemäßen Verfahrens zum Betrieb der einzelnen Systemkomponenten veranlaßt wird.

Im folgenden werden nicht einschränkend zu verstehenden Ausführungsbeispiele z.T. anhand der Zeichnung besprochen. In dieser zeigen:

Fig. 1 schematisch den Informationsfluß bei einer elektronischen Wahl,

Fig. 2 schematisch den Informationsfluß bei einer elektronischen Wahl in Form einer Internetkorrespondenszwahl,

Fig. 3 ein elektronisches Stimmeingabe-Panel,

Fig. 4 eine elektronische Wahlkabine, und

Fig. 5 eine Vorrichtung zur Identifikation und Authentisierung unter Verwendung digitalen Signaturen,

alles entsprechend der vorliegenden Erfindung.

Fig. 1 zeigt schematisch den Informationsfluß bei einer elektronischen Wahl in Form einer öffentlich kontrollierten Internetwahlkabinenwahl. Hierzu könnte folgendes Übertragungsprotokoll genutzt werden.

Für die folgenden Figuren gelten beispielhaft diese Nomenklaturvereinfachungen für die Verschlüsselungsverfahren, die Signaturen und die Statuskennzeichen:

W_{priv}	:privater Schlüssel des Wählers;
W_{pub}	:öffentlicher Schlüssel des Wählers;
V_{priv}, V_{pub}	:privater und öffentlicher Schlüssel des Validators
P_{priv},P_{pub}	:privater und öffentlicher Schlüssel des Psephor; Urnenserver (*)
E_{priv}, E_{pub}	:privater und öffentlicher Schlüssel des Wahlvorstand, Wahl
A_{priv}, A_{pub}	:privater und öffentlicher Schlüssel der anonymen Identität des Wählers

Zufallszahlen:

n,m	:Blindingsfaktoren
idw	:Wahlberechtigungsnummer eines Wählers
wtoken	:Wahlscheinnummer für einen ausgegebenen Wahlschein

Validator

Der Wahlamtserver enthält als elektronisches Wählerverzeichnis die Datei „Wählerverzeichnis Wahlkreis XX“ mit folgenden Feldern:

F_V_Wpub	: öffentlicher Schlüssel des Wählers
F_V_Wl	: Wahllokalnummer
F_V_WS	: Wahlstatus beim Validator
F_V_Wpriv_ Wkontrolle	: signierterWahlkontrollstring Wpriv(wkontrolle)
F_V_AV_WS_2	: Anzahl der Wahlversuche bei F_V_WS=2
F_V_AV_WS_3	: Anzahl der Wahlversuche bei F_V_WS=3

F_V_AV_WS_6	: Anzahl der Wahlversuche bei F_V_WS=6
F_V_AV_WS_7	: Anzahl der Wahlversuche bei F_V_WS=7
F_V_AV_WS_10	: Anzahl der Wahlversuche bei F_V_WS=10

Name	: Nachname des Wählers
Vorname	: Vorname
Straße	: Straßenname + Hausnummer
PLZ	: Postleitzahl
Ort	: Ort
Geb_datum	: Geburtsdatum
PAN	: Personalausweisnummer

Für die Korrespondenzwahl wird eine Tokenliste(TL) geführt :

F_TL_wtoken	: wtoken
F_TL_WS	:Wahlstatus des wtoken ; 0 - nicht benutzt
W_{pub}	:öffentlicher Schlüssel des Wählers, an dem wtolken vergeben wurde; (wpub ist nur während des Wahlvorganges temporär gespeichert, bei erfolgreicher Wahl wird der Wert von 10 = gewählt überschrieben.

Die UrnenDatei WL hat folgende Struktur:

Wtoken	:Wahlscheinkennung
E_{pub}(wahlschein(x))	:Mit dem öffentlichen Schlüssel des Wahlvorstandes verschlüsseltes Wählervotum

Die Urnenkontrolldatei enthält folgende Felder:

F_P_Apub	: öffentlicher Schlüssel der anonymen Identität des Wählers (A_{pub})
F_P_Wtoken	: Wahlscheinkennung (wtoken)
F_P_WL	: Wahllokalnummer (Wl)
F_P_Apriv	: Feld der anonymen Identität signiertes Wählervotum und Wahlscheinkennung; (A_{priv}(E_{pub}(wahlschein(x), wtoken)
F_P_Vpriv scheinkennung	:der vom Validator signierte Hashwert des Votum, der Wahl- V_{priv}(hash(E_{pub}(wahlschein(x)),wtoken)

F_P_Apriv_wkontrolle	:mit dem privaten Schlüssel der anonymen Identität signierte Wahlkontrollstring A_{priv}(wkontrolle) oder A_{priv}(hash(wkontrolle)
F_P_WS	:Wahlstatus beim Psephor
F_P_AV_WS_4	: Anzahl der Wahlversuche bei F_P_WS=4
F_P _AV_WS_5	: Anzahl der Wahlversuche bei F_P_WS=5
F_P _AV_WS_8	: Anzahl der Wahlversuche bei F_P_WS=8
F_P _AV_WS_9	: Anzahl der Wahlversuche bei F_P_WS=9

WtokenListe

F_P_Wtoken	: wtoken (Wahlscheinkennung)
F_P_Status	: 0 – nicht benutzt; (1 – ausgegeben)

Je nachdem, ob die Wahl von einem öffentlich kontrollierten Eingabestation (Wahlkabine, öffentliches Terminal) oder von einer privaten Eingabestation (PC o.ä.) erfolgt, kann der Systemdurchlauf variiert werden. In Abhängigkeit von dem Wahlanlaß und Wahlkontext , können die Sicherheitsanforderungen verändert werden und das Protokoll variiert werden. Die elektronische Wahl findet in 11 Phasen statt:

Phase 0 : Der Verbindungsaufbau Pollster/Validator

Das transferierte Datenpaket **Nachricht** 0 enthält Informationen zum Aufbau einer SSL-Verbindung zwischen Pollster und Validator

Phase 1 : Übertragung eines Datenpaketes von Validator an Pollster:

1. Der Validator erzeugt einen zufälligen Wahlkontrollstring, nämlich wkontrolle.
2. Es wird der hash-Wert des Wahlkontrollstrings errechnet, also hash(wkontrolle).
3. Der hash-Wert des Wahlkontrollstrings wkontrolle wird mit dem privaten Schlüssel des Wahlamtes V_{priv} verschlüsselt und signiert, es ergibt sich V_{priv}(hash(wkontrolle))
4. Der öffentliche Schlüssel des Wahlamtes V_{pub}, der Wahlkontrollstring und der signierte hash-Wert werden als Nachricht 1 vom Validator zum Pollster übertragen.

Das Datenpaket **Nachricht 1** enthält : (V_{priv}(hash(wkontrolle));wkontrolle;V_{pub})

Phase 2 : Übertragung eines Datenpaketes von Pollster an Validator:

1. Der Pollster prüft die Identität des Validators.
2. Der Pollster überprüft mittels der hash-Funktion die Korrektheit der Übertragung.
3. Er signiert mit dem privaten Schlüssel des Wählers W_{priv} den Wahlkontrollstring wkontrolle.
4. Er verschlüsselt den signierten Wahlkontrollstring und die Wahlberechtigungsnummer des Wählers idw der Wahlanmeldung w mit dem öffentlichen Schlüssel des Wahlamts.

Das Datenpaket **Nachricht 2** enthält somit: V_{pub}(W_{priv}(wkontrolle); W_{pub})

Phase 3 : Übertragung eines Datenpaketes von Validator an Pollster:

1. Der Validator prüft die Identität und Wahlberechtigung des Wählers.

- Ist der Wähler nicht wahlberechtigt folgt: Fehlerroutine 1 (**Nicht wahlberechtigt**). Ist der Wähler wahlberechtigt folgt die Überprüfung der digitalen Signatur Wpriv(wkontrolle) durch den Validator.
- Schlägt die Authentifizierung fehl folgt : Fehlerroutine 2 (**keine gültige Signatur**).

  Andernfalls überprüft der Validator den Wahlstatus (F_V_WS). Folgende Statuskennzeichen können vorliegen:

  F_V_WS =10: Nachricht „schon gewählt"

  F_V_WS >0 und <10 : Der Wahlvorgang hat schon begonnen ist aber noch nicht beendet.

  F_V_WS =0: Beginn des Wahlvorganges

2. Die Statuskennzahl wird auf Beginn des Wahlvorganges gesetzt: F_V_WS = 1

3. Es wird der hash-Wert der Wahlunterlagen Wahlschein (wahlschein), öffentlicher Schlüssels des Psephors (Ppub) und öffentlicher Schlüssel des Wahlvorstandes (Epub) gebildet: hash(wahlschein,Ppub,Epub)
4. Dieser hash-Wert wird vom Wahlamt mit Vpriv signiert Vpriv(hash(wahlschein,Ppub,Epub))
5. Der signierte hash-Wert und die Wahlunterlagen (wahlschein, Ppub, Epub) werden mit dem öffentlichen Schlüssel des Wählers verschlüsselt und als Nachricht vom Validator zum Pollster geschickt.

Das Datenpaket **Nachricht 3** enthält somit: W_{pub}(Vpriv(hash(wahlschein, P_{pub}, E_{pub}));wahlschein; P_{pub}; E_{pub})

Phase 4 : Übertragung eines Datenpaketes von Pollster an Psephor:

1. Der Pollster entschlüsselt die Nachricht und überprüft die Korrektheit.
2. Er überprüft die Identität von der Signaturen und Verschlüsselungen P_{pub} und E_{pub}.
3. Der Pollster erzeugt ein zufälliges Schlüsselpaar als anonyme Identität (A_{priv}, A_{pub})
4. Er signiert den öffentlichen Schlüssel der anonymen Identität und den Wahlkontrollstring mit dem privaten Schlüssel der anonymen Identität A_{priv}(wkontrolle, A_{pub}).
5. Der signierte öffentlicher Schlüssel und der Wahlkontrollstring und der öffentliche Schlüssel der anonymen Identität werden mit dem öffentlichen Schlüssel des Psephors verschlüsselt und als Nachricht vom Pollster zum Psephor gesandt.

Das Datenpaket **Nachricht 4** enthält somit: P_{pub} (A_{priv} (wkontrolle,A_{pub}); wkontrolle,A_{pub})

Phase 5 : Übertragung eines Datenpaketes von Pspehor an Pollster:

1. Der Psephor entschlüsselt die Nachricht 4 und überprüft diese auf Korrektheit.

2. Der Psephor vergibt für A_{pub} ein eindeutiges k-stelliges Wahlscheinkennung(wtoken). Es werden folgende Feldwerte gesetzt:
   - $F\_P\_A_{pub} = A_{pub}$
   - F_P_WS = 3 (A_{pub} empfangen)
   - F_P_wtoken = wtoken
   - $F\_P\_A_{priv} = A_{priv}$(wkontrolle)
3. Er signiert die Wahlscheinkennung mit seinem privaten Schlüssel Ppriv(wtoken) und verschlüsselt diese Werte mit dem öffentlichen Schlüssel der anonymen Identität A_{pub}. Der Psephor schickt diese Nachricht zum Pollster.

Das Datenpaket **Nachricht 5** enthält somit: $A_{pub}(P_{priv}$(wtoken);wtoken;)

4. F_P_WS = 4 (Wahlscheinkennung versandt)

Phase 6 : Übertragung eines Datenpaketes von Pollster an Validator:

1. Der Pollster entschlüsselt die **Nachricht 5** und überprüft die Korrektheit der Übertragung.
2. Der Wähler füllt den Wahlschein aus : wahlschein(x) ist der ausgefüllte Wahlschein.
3. Der ausgefüllte Wahlschein wahlschein(x) wird mit dem öffentlichen Schlüssel des Wahlvorstandes E_{pub} verschlüsselt: E_{pub}(wahlschein(x))
4. Der Pollster hasht die verschlüsselte Wahl zusammen mit dem wtoken: hash(E_{pub}(wahlschein(x),wtoken)
5. Der Pollster blindet diesen hash-Wert von Epub(wahlschein(x)) und Wahlscheinnummer (wtoken): blind(m,hash(E_{pub}(wahlschein(x)),wtoken))
6. Dieser geblindete Wert wird mit dem privaten Schlüssel des Wählers signiert: Wpriv(blind(m, hash(E_{pub}(wahlschein(x)),wtoken)))
7. Der signierte geblindete und gehashte Wert des verschlüsselten Wahlvotums und der Wahlscheinnummer und der geblindete Wert selbst werden mit dem öffentlichen

Schlüssel des Wahlamtes verschlüsselt und als Nachricht vom Pollster an den Validator gesandt.

Das Datenpaket **Nachricht 6** enthält somit:
$V_{pub}(W_{priv}$(blind (m, hash (E_{pub}(wahlschein(x)),wtoken))); blind(m, hash (Epub(wahlschein(x)), wtoken)))

Phase 7 : Übertragung eines Datenpaketes von Validator an Pollster:

1. Der Validator entschlüsselt die **Nachricht 6** und prüft die Korrektheit .
2. Er signiert die geblindete,gehashte Wahlentscheidung und Wahlscheinkennung, und die Wahllokalnummer des Wählers (WL).
3. Die signierten gehashten geblindeten Werte, die geblindeten Werte und die Wahllokalnummer werden mit dem öffentlichen Schlüssel des Wählers zum Pollster zurückgesandt.

Das Datenpaket **Nachricht 7** enthält somit:
$W_{pub}(V_{priv}$(blind(m, hash(E_{pub}(wahlschein(x)),wtoken)), WL); blind(m, hash(E_{pub} (wahlschein(x)), wtoken)); WL)

Phase 8 : Übertragung eines Datenpaketes von Pollster an Psephor:

1. Der Pollster entschlüsselt die **Nachricht 7** und prüft die digitale Signatur und Korrektheit.
2. Er entblindet die signierte geblindete Wahlentscheidung und Wahlscheinnummer. Unblind (m, V_{priv} (blind (m, hash (E_{pub} (wahlschein(x)), wtoken)))) = V_{priv}(hash (E_{pub} (wahlschein(x)), wtoken))
3. Der Pollster bildet zur Wahlbestätigung durch den Psephor: blind(n, hash(W_{pub}(A_{pub}))
4. Der Pollster signiert die verschlüsselte Wahlentscheidung, Wahlscheinnummer und Wahllokalnummer. Die vom Wahlamt und von der anonymen Identität signierten

Werte werden mit dem öffentlichen Schlüssel des Psephors verschlüsselt und zum Psephor gesandt.

Das Datenpaket **Nachricht 8** enthält somit: $P_{pub}(V_{priv}(hash(E_{pub}(wahlschein(x)); wtoken), WL); A_{priv}(E_{pub}(wahlschein(x),wtoken,WL); wtoken)$

Phase 9 : Übertragung eines Datenpaketes von Psephor an Pollster:

1. Der Psephor entschlüsselt die **Nachricht 8.**
2. Pspehor setzt F_P_WS = 8 (Wahlvotum empfangen)
3. Die Signatur des Wahlamtes wird mit V_{pub}, die Signatur der anonymen Identität wird mit A_{pub} überprüft.
4. Durch Vergleich der resultierenden Werte wird die Korrektheit des empfangenen Votums gesichert.
5. Der Psephor legt die E_{pub}(wahlschein(x) und die Wahlscheinnummer in die Urne WL
6. In der wtoken-Liste wird der Status auf 2 = „in Urne gelegt" gesetzt
7. In der Wahlkontrolldatei werden zu Kontrollzwecken gespeichert:
   - F_P_WL = WL
   - $F\_P\_V_{priv} = V_{priv}(E_{pub}$(wahlschein(x), wtoken, WL)
   - $F\_P\_A_{priv} = A_{priv}(E_{pub}$(wahlschein(x), wtoken, WL)
8. F_P_WS = 9 (Wahlschein in Urne)
9. Der Psephor erzeugt eine eindeutige Wahlkontrollzahl i
10. Dieser signierte Wahlbestätigung wird vom Psephor mit dem öffentlichen Schlüssel der anonymen Identität zum Pollster geschickt.

Das Datenpaket **Nachricht 9** enthält somit: A_{pub} (P_{priv}(Wahlbestätigung); Wahlbestätigung)

Phase 10 : Übertragung eines Datenpaketes von Pollster an Validator:

1. Der Pollster entschlüsselt und prüft die Korrektheit der **Nachricht 9**.
2. Die Wahlkontrollzahl i wird dem Wähler ausgegeben.
3. Der Pollster leitet diese Nachricht als Wahlbestätigung signiert und verschlüsselt an den Validator weiter

Das Datenpaket **Nachricht 10** enthält somit: $V_{pub}(W_{priv}\ (P_{priv}(\text{wahlbestätigung});\ W_{pub});$ wahlbestätigung; $W_{pub})$

Phase 11 : Übertragung eines Datenpaketes von Validator an Pollster

1. Der Validator entschlüsselt und prüft die Korrektheit der Nachricht 10.
2. Der Wahlstatus beim Validator wird auf „10 = gewählt" gesetzt.
3. Der Validator erzeugt eine Wahlkontrollzahl i
4. Der Validator schickt die Wahlbestätigung mit der Wahlkontrollzahl i

Das Datenpaket **Nachricht 11** enthält somit : $W_{pub}\ (V_{priv}(P_{priv}(\text{wahlbestätigung}),\ i);$ wahlbestätigung; i)

5. Der Pollster prüft die Nachricht
6. Die Wahlbestätigung und die Wahlkontrollzahl i auf dem Eingabemonitor mitgeteilt und/oder ausgedruckt.

Fig. 2 zeigt schematisch den Informationsfluß der elektronischen Wahl in Form einer Internetkorrespondenszwahl. Bei dieser Form der Wahl entfallen die öffentlichen Wahlkabinen. Die Wahl kann an jedem mit dem Internet verbundenen Pc durchgeführt werden.

Vorphase: Der Psephor erzeugt vor der Wahl eine Liste von k-stelligen Wahltoken (Wahlscheinkennungen) und schickt diese verschlüselt an den Validator. (Sie kann auch - auf ein Medium gespeichert - zum Validator gebracht werden.) Wobei TL die Tokenliste darstellt (jedes Wahltoken ist zusätzlich verschlüsselt).

Das Datenpaket enthält folgende Informationen: $V_{pub}(P_{priv}(hash(TL)), TL)$

Der Validator bestätigt hierauf den Erhalt der Liste mit dem Datenpaket: $P_{pub}(V_{priv}(hash(TL)),TL)$

Phase 0 : Verbindungsaufbau Pollster/Validator

Das Datenpaket **Nachricht 0** enthält Informationen zum Aufbau einer SSL-Verbindung zwischen Pollster und Validator.

Phase 1 : Übertragung eines Datenpaketes von Validator an Pollster:

1. Der Validator erzeugt einen zufälligen Wahlkontrollstring (wkontrolle)
2. Es wird der hash-Wert des Wahlkontrollstrings errechnet: hash(wkontrolle)
3. Der hash-Wert des Wahlkontrollstrings wkontrolle wird mit dem privaten Schlüssel des Wahlamtes Vpriv verschlüsselt und signiert:
4. $V_{priv}(hash(wkontrolle))$
5. Der öffentliche Schlüssel des Wahlamtes V_{pub}, der Wahlkontrollstring und der signierte hash-Wert werden als **Nachricht 1** vom Validator zum Pollster übertragen

Das Datenpaket **Nachricht 1** enthält somit : $(V_{priv}(hash(wkontrolle));wkontrolle;V_{pub})$

Phase 2 : Übertragung eines Datenpaketes von Pollster an Validator:

1. Der Pollster prüft die Identität des Validators.
2. Der Pollster überprüft mittels der hash-Funktion die Korrektheit der Übertragung
3. Er signiert mit dem privaten Schlüssel des Wählers W_{priv} den Wahlkontrollstring wkontrolle.

4. Er verschlüsselt den signierten Wahlkontrollstring und seinen öffentlichen Schlüssel mit dem öffentlichen Schlüssel des Wahlamts.
5. Diese Nachricht schickt der Pollster an den Validator.

Das Datenpaket **Nachricht 2** enthält somit: $V_{pub}(W_{priv}(wkontrolle); W_{pub})$

Phase 3 : Übertragung eines Datenpaketes von Validator an Pollster:

1. Der Validator prüft die Identität und Wahlberechtigung des Wählers

   Ist Wähler nichtwahlberechtigt : Fehlerroutine 1 **(Nicht wahlberechtigt)**

   Schlägt die Authentifizierung fehl: Fehlerroutine 2 **(keine gültige Signatur)**

   Andernfalls : Überprüfung des Wahlstatus (F_V_WS)

- Falls F_V_WS =10 : Nachricht „schon gewählt"

  Falls F_V_WS >0 und <10 : Der Wahlvorgang hat schon begonnen ist aber noch nicht beendet.

- Falls F_V_WS =0 : Beginn des Wahlvorganges

2. Die Wahlstatuskennzahl wird auf 1 gesetzt. Die Wahl beginnt; F_V_WS = 1
3. Es wird der hash-Wert der Wahlunterlagen(Wahlschein (wahlschein), öffentlicher Schlüssels des Psephors (P_{pub}) und öffentlicher Schlüssel des Wahlvorstandes (E_{pub}) gebildet: hash(wahlschein,P_{pub},E_{pub})
4. Dieser hash-Wert wird vom Wahlamt mit V_{priv} signiert; V_{priv} (hash(wahlschein, wtoken, P_{pub},E_{pub}))
5. Der signierte hash-Wert und Wahlunterlagen (wahlschein, wtpken, P_{pub}, E_{pub}) werden mit dem öffentlichen Schlüssel des Wählers verschlüsselt und als Nachricht vom Validator zum Pollster geschickt.
6. Beim Validator wird in die Liste TL das Statusfeld des wtokwn auf idw für die Dauer des Wahlvorganges gesetzt.

Das Datenpaket **Nachricht 3** enthält somit: $W_{pub}(V_{priv}$ (hash (wahlschein, wtoken, P_{pub}, E_{pub})); wahlschein; wtoken, P_{pub}; E_{pub})

Phase 4 : Übertragung eines Datenpaketes von Pollster an Validator:

1. Der Pollster entschlüsselt die Nachricht und überprüft die Korrektheit der Übertragung.
2. Der Wähler füllt den Wahlschein aus : wahlschein(x) ist der ausgefüllte Wahlschein.
3. Der ausgefüllte Wahlschein wahlschein(x) wird mit dem öffentlichen Schlüssel des Wahlvorstandes E_{pub} verschlüsselt: Epub(wahlschein(x))
4. Der Pollster hashed E_{pub}(wahlschein(x)) und die Wahlscheinnummer wtoken und blinded sie mit einem zufälligen Blindingsfaktor m : blind(m, hash(Epub(wahlschein(x)), wtoken))
5. Dieser Wert wird mit dem privaten Schlüssel des Wählers signiert:
6. W_{priv}(blind(m, hash(E_{pub}(wahlschein(x)), wtoken))
7. Der signierte geblindete und gehashte Wert des verschlüsselten Wahlvotums und der Wahlscheinnummer und der geblindete Wert selbst werden mit dem öffentlichen Schlüssel des Wahlamtes verschlüsselt und als Nachricht vom Pollster an den Validator gesandt.

Das Datenpaket **Nachricht 4** enthält somit: $V_{pub}(W_{priv}$(blind(n, hash(E_{pub}(wahlschein(x)), wtoken))); blind(n, hash(Epub(wahlschein(x)), wtoken)))

Phase 5 : Übertragung eines Datenpaketes von Validator an Pollster:

1. Der Validator entschlüsselt die **Nachricht 4** und prüft die Korrektheit.
2. Er signiert die geblindete Wahlentscheidung und Wahlscheinkennung, und die Wahllokalnummer des Wählers (WL).
3. Die signierten geblindeten hash-Werte, der geblindeten hash-Werte und

4. die Wahllokalnummer werden mit dem öffentlichen Schlüssel des Wählers verschlüsselt zum Pollster zurückgesandt.

Das Datenpaket **Nachricht 5** enthält somit: $W_{pub}(V_{priv}(blind(m, hash(E_{pub}(wahlschein(x)), wtoken)), WL); blind(m, hash(E_{pub}(wahlschein(x)), wtoken); WL))$

Phase 6 : Übertragung eines Datenpaketes von Pollster an Psephor:

1. Der Pollster entschlüsselt die Nachricht und prüft die digitale Signatur und Korrektheit der Nachricht.
2. Er entblindet die signierte geblindete gehashte Wahlentscheidung und Wahlscheinnummer.
3. Der Pollster signiert die verschlüsselte Wahlentscheidung, Wahlscheinnummer, Wahlkreis-/Wahllokalnummer.
4. Die vom Wahlamt und von der anonymen Identität signierten Werte V_{priv} (hash(E_{pub}(wahlschein(x), wtoken), WL) und A_{priv}(Epub(wahlschein(x), wtoken, WL) werden mit dem öffentlichen Schlüssel des Psephors verschlüsselt und zum Psephor gesandt. Diese Nachricht wird als Mail mit einer anonymisierten, u.U. fiktiven AbsenderIP versehen, die der Server über eine Firewall kontrollieren kann.

Das Datenpaket **Nachricht 6** enthält somit: $P_{pub}(V_{priv}(hash(E_{pub}(wahlschein(x)),wtoken), WL); A_{priv}(E_{pub}(wahlschein(x)); wtoken,WL);A_{pub})$

Phase 7 : Übertragung eines Datenpaketes von Psephor an Validator

1. Der Psephor entschlüsselt die Nachricht.
2. Die Signatur des Wahlamtes wird mit V_{pub} überprüft, die Signatur der anonymen Identität wird mit A_{pub} überprüft.
3. Pspehor setzt die Wahlstatuskennzahl auf F_P_WS = 8 (Wahlvotum empfangen).

4. Durch Vergleich der resultierenden Werte wird die Korrektheit des empfangenen Votums gesichert.
5. Es wird geprüft ,ob wtoken aus der Wahltokenliste TL stammt.
6. Der Psephor legt die E_{pub}(wahlschein(x)) und die Wahlscheinnummer in die Urne WL.
7. In der wtoken-Liste wird der Status des wtoken auf 2 =„in Urne gelegt“ gesetzt.
8. In der Wahlkontrolldatei werden zu Kontrollzwecken gespeichert:
   - F_P_WL = WL
   - F_P_V_{priv} = V_{priv}(hash(E_{pub}(wahlschein(x), ,wtoken), WL)
   - F_P_A_{priv} = A_{priv}(E_{pub}(wahlschein(x), wtoken, WL)

   (Die Felder F_P_wtoken = wtoken und F_P_Apub = Apub sind schon gespeichert)
9. Die Wahlstatuskennzahl F_P_WS wird auf 9 gesetzt. (Wahlschein in Urne)
10. Der Psephor signiert die Wahlbestätigung.
11. Diese Nachricht wird vom Psephor signiert mit dem öffentlichen Schlüssel des Validators zum Validator geschickt.

Das Datenpaket **Nachricht 7** enthält somit: V_{pub} (P_{priv}(wtoken), wahlbestätigung); wtoken; wahlbestätigung)

Phase 8 : Übertragung eines Datenpaketes von Validator an Pollster

1. Der Validator entschlüsselt und prüft die Korrektheit der **Nachricht 7.**
2. Der Wahlstatus von wtoken (= idw) wird in der Liste der Wahltoken wird auf 2 (= „in Urne“) gesetzt. Der Wahlstatus beim Validator wird auf „10 = gewählt“ gesetzt.
3. Der Validator bildet eine Wahlkontrollzahl i und leitet die Wahlbestätigung und die Wahlkontrollzahl weiter an den Pollster weiter:

Das Datenpaket **Nachricht 8** enthält somit: W_{pub} (V_{priv} (wahlbestätigung, i); P_{priv} (wahlbestätigung, i);)

Phase 9 : Übertragung eines Datenpaketes von Psephor an den Validator

1. Nach Beendigung der Wahl und nach Konsistenzüberprüfungen wird die Urnendatei an den Validator übermittelt. $V_{pub}(P_{priv}(Urne\_XX), Urne\_XX)$
2. Die Voten werden durch den Wahlvorstand mittels E_{priv} entschlüsselt und ausgezählt.
3. Nach der Auszählung werden die Stimmen bekannt gegeben und mittels Internet an die Wahlleiter übermittelt.

Fig. 3 zeigt ein elektronisches Stimmeingabe Panel 1. Dies ist ein vorzugsweise in der öffentliche Wahlkabine eingerichtetes Panel, welches mit Hilfe biometrischer Messung eine Eindeutige Identifikation des Benutzers zulässt. Auf dem Panel sind hierzu Sensorfelder 2 angebracht.

Fig. 4 zeigt eine elektronische Wahlkabine 3 mit dem elektronische Stimmeingabe-Panel 1. Diese elektronische Wahlkabine 3 ist direkt mit dem Wahlnetzwerk verbunden und ermöglicht so die direkte und einfache Abwicklung der Wahl.

Fig. 5 zeigt eine Vorrichtung zur Identifikation und Authentisierung unter Verwendung digitalen Signaturen. Hierzu wird das Sensorfeld 2 zur Aufnahme der biometrischen Messung und eine Chipkarte 4, auf welcher Personal- und Verwaltungsdaten stehen benötigt.

Titel: Telekommunikationsprotokoll, -system und -vorrichtungen zur anonymen und authentischen Abwicklung einer elektronischen Wahl

Patentansprüche

1. Telekommunikationsprotokoll zur anonymen und authentischen Abwicklung einer elektronischen Wahl, wobei

   von einer elektronischen Wahlstelle ein elektronischer Wahlschein von einem elektronischen Wahlleiter angefordert wird,

   der elektronische Wahlleiter die Berechtigung eines die elektronische Wahlstelle verwendenden Wählers zur Teilnahme an der elektronischen Wahl prüft und im Falle der Feststellung der Berechtigung des die elektronische Wahlstelle verwendenden Wählers zur Teilnahme an der elektronischen Wahl einen elektronischen Wahlschein an die Wahlstelle sendet,

   die elektronische Wahlstelle den vom elektronischen Wahlleiter empfangenen elektronischen Wahlschein mit einer von einem Wähler elektronisch getroffenen Wahl versieht, und

die elektronische Wahlstelle den mit der Wahl versehenen elektronischen Wahlschein an einen elektronischen Wahlrechner zur Sammlung und/oder Auswertung sendet,

dadurch gekennzeichnet, daß

die der Person des Wählers eindeutig zugeordneten Daten und die von dem Wähler getroffene elektronische Wahl in allen Phasen der Verarbeitung oder Übertragung entweder

- voneinander getrennt oder
- verschlüsselt oder
- voneinander getrennt und verschlüsselt

vorliegen.

2. Telekommunikationsprotokoll zur anonymen und authentischen Abwicklung einer elektronischen Wahl nach Anspruch 1, dadurch gekennzeichnet, daß

die elektronische Wahlstelle den elektronischen Wahlschein mit der getroffenen Wahl und mit einer dem Wähler zugeordneten Kennung versehen, verschlüsselt an den elektronischen Wahlleiter zurücksendet,

der elektronische Wahlleiter den an ihn zurückgesandten verschlüsselten elektronischen Wahlschein signiert und dann wieder so von ihm signiert an die elektronische Wahlstelle sendet,

die elektronische Wahlstelle den mit der Wahl versehenen und von dem elektronischen Wahlleiter signierten elektronischen Wahlschein wieder entschlüsselt, die dem Wähler zugeordnete Kennung entfernt und den elektronischen Wahlschein im Falle seiner Authentizität ohne die Kennung aber mit Signatur an den elektronischen Wahlrechner zur Sammlung und/oder Auswertung sendet.

3. Telekommunikationsprotokoll zur anonymen und authentischen Abwicklung einer elektronischen Wahl nach Anspruch 2, dadurch gekennzeichnet, daß die dem Wähler zugeordnete Kennung eine den Wähler identifizierende Identifikation ist.

4. Telekommunikationsprotokoll zur anonymen und authentischen Abwicklung einer elektronischen Wahl nach Anspruch 2, dadurch gekennzeichnet, daß die dem Wähler zugeordnete Kennung diesem anonym zugeordnet wird und so keine Identifikation des Wählers darstellt.

5. Telekommunikationsprotokoll zur anonymen und authentischen Abwicklung einer elektronischen Wahl nach einem der Ansprüche 2 bis 4 dadurch gekennzeichnet, daß die elektronische Wahlstelle den mit der Wahl versehenen und von dem elektronischen Wahlleiter signierten elektronischen Wahlschein wieder entschlüsselt, die dem Wähler zugeordnete Kennung entfernt und den elektronischen Wahlschein ohne die Kennung aber mit Signatur an den elektronischen Wahlrechner zur Sammlung und/oder Auswertung nur dann sendet, wenn die elektronische Wahlstelle die Authentizität des signierten elektronischen Wahlscheins derart feststellt, daß die dem Wähler zugeordnete Kennung nach Empfang vom elektronischen Wahlleiter der Kennung entspricht, wie sie von der elektronischen Wahlstelle an den elektronischen Wahlleiter gesendet wurde.

6. Telekommunikationsprotokoll zur anonymen und authentischen Abwicklung einer elektronischen Wahl nach einem der Ansprüche 2 bis 5 dadurch gekennzeichnet, daß die elektronische Wahlstelle den mit der Wahl versehenen und von dem elektronischen Wahlleiter signierten elektronischen Wahlschein wieder entschlüsselt, die dem Wähler zugeordnete Kennung entfernt und den elektronischen Wahlschein ohne die Kennung aber mit Signatur an den elektronischen Wahlrechner zur Sammlung und/oder Auswertung nur dann sendet, wenn die elektronische Wahlstelle die Authentizität des signierten elektronischen Wahlscheins derart feststellt, daß die vom Wähler getroffene Wahl der Wahl entspricht, wie sie von der elektronischen Wahlstelle an den elektronischen Wahlleiter gesendet wurde.

7. Telekommunikationsprotokoll zur anonymen und authentischen Abwicklung einer elektronischen Wahl nach einem der Ansprüche 2 bis 6 dadurch gekennzeichnet, daß auf dem elektronischen Wahlrechner elektronische Wahlscheine nur gesammelt nicht jedoch ausgewertet werden.

8. Telekommunikationsprotokoll zur anonymen und authentischen Abwicklung einer elektronischen Wahl nach Anspruch 7 dadurch gekennzeichnet, daß die vom elektronischen Wahlrechner gesammelten elektronischen Wahlscheine an den elektronischen Wahlleiter zur Auswertung gesendet werden.

9. Telekommunikationsprotokoll zur anonymen und authentischen Abwicklung einer elektronischen Wahl nach einem der Ansprüche 2 bis 8 dadurch gekennzeichnet, daß nur solche elektronischen Wahlscheine gesammelt und/oder ausgewertet werden, die auch vom elektronischen Wahlleiter signiert sind.

10. Telekommunikationsprotokoll zur anonymen und authentischen Abwicklung einer elektronischen Wahl nach einem der Ansprüche 2 bis 9 dadurch gekennzeichnet, daß die Auswertung der elektronischen Wahlscheine in Form einer Zählung, vorzugsweise nach Wahlkategorien, der jeweils getroffenen Wahl erfolgt.

11. Telekommunikationsprotokoll zur anonymen und authentischen Abwicklung einer elektronischen Wahl nach einem der Ansprüche 1 bis 10, dadurch gekennzeichnet, daß mindestens eines der verwendeten Verschlüsselungsverfahren ein Blinding-Verfahren ist.

12. Telekommunikationsprotokoll zur anonymen und authentischen Abwicklung einer elektronischen Wahl nach einem der Ansprüche 1 bis 11, dadurch gekennzeichnet, daß mindestens eines der verwendeten Verschlüsselungsverfahren ein RSA-Verschlüsselungsverfahren ist.

13. Telekommunikationsprotokoll zur anonymen und authentischen Abwicklung einer elektronischen Wahl nach einem der Ansprüche 1 bis 12 dadurch gekennzeichnet, daß Daten über eine Hashfunktion gesichert übertragen werden.

14. Elektronisches Wahlsystem zur Durchführung einer elektronischen Wahl mit mindestens einem elektronischen Wahlleiter (Validator), vorzugsweise einem ersten Server-Rechner-System, mindestens einem elektronischen Wahlrechner (Psephor, Urne) vorzugsweise einem zweiten Server-Rechner-System, und mindestens einer elektronischen Wahlstelle (Pollster), vorzugsweise einem Client-Rechner-System, wobei die elektronische Wahlstelle mit dem elektronischen Walleiter und dem elektronischen Wahlrechner, vorzugsweise über ein Telekommunikationsnetzwerk, verbunden ist und das elektronische Wahlsystem programmtechnisch so eingerichtet ist, daß es nach dem Telekommunikationsprotokoll zur anonymen und authentischen Abwicklung einer elektronischen Wahl nach einem der Ansprüche 1 bis 13 arbeitet.

15. Elektronisches Wahlsystem zur Durchführung einer elektronischen Wahl nach Anspruch 14, dadurch gekennzeichnet, daß der elektronische Wahlleiter und der elektronischer Wahlrechner auf dem gleichen Rechner-System, vorzugsweise einem Server-Rechner-System, vorliegen.

16. Elektronischer Wahlleiter (Validator), vorzugsweise ein Server-Rechner-System, welcher, vorzugsweise über ein Telekommunikationsnetzwerk, mit mindestens einer elektronischen Wahlstelle (Pollster), vorzugsweise einem Client-Rechner-System, verbunden ist, und der elektronische Wahlleiter programmtechnisch so eingerichtet ist, daß er die Berechtigung eines die elektronische Wahlstelle verwendenden Wählers zur Teilnahme an einer elektronischen Wahl prüft, dadurch gekennzeichnet, daß

    die der Person des Wählers eindeutig zugeordneten Daten und die von dem Wähler getroffene elektronische Wahl in allen Phasen der Verarbeitung auf dem elektronischen Wahlleiter oder Übertragung zum oder vom elektronischen Wahlleiter entweder

    - voneinander getrennt oder
    - verschlüsselt oder
    - voneinander getrennt und verschlüsselt

    vorliegen.

17. Elektronischer Wahlleiter (Validator) nach Anspruch 16, dadurch gekennzeichnet, daß dieser programmtechnisch so eingerichtet ist, daß er die Berechtigung eines eine elektronische Wahlstelle verwendenden Wählers zur Teilnahme an einer elektronischen Wahl prüft und im Falle der Feststellung der Berechtigung des die elektronische Wahlstelle verwendenden Wählers zur Teilnahme an der elektronischen Wahl einen elektronischen Wahlschein an die Wahlstelle sendet und der elektronische Wahlleiter einen an ihn von der elektronischen Wahlstelle zurückgesandten verschlüsselten elektronischen Wahlschein signiert und dann wieder so von ihm signiert an die elektronische Wahlstelle sendet.

18. Elektronischer Wahlrechner (Psephor, Urne), vorzugsweise ein Server-Rechner-System, welcher, vorzugsweise über ein Telekommunikationsnetzwerk, mit mindestens einer elektronischen Wahlstelle (Pollster), vorzugsweise einem Client-Rechner-System, verbunden ist, wobei der elektronische Wahlrechner programmtechnisch so eingerichtet ist, daß er eine Sammlung und/oder Auswertung der, an ihn von der elektronischen Wahlstelle gesendeten elektronischen Wahlscheine vornimmt, dadurch gekennzeichnet, daß

    die der Person des Wählers eindeutig zugeordneten Daten und eine vom Wähler getroffene elektronische Wahl in allen Phasen der Verarbeitung auf dem elektronischen Wahlrechner oder Übertragung zum oder vom elektronischen Wahlleiter entweder

    - voneinander getrennt oder
    - verschlüsselt oder
    - voneinander getrennt und verschlüsselt

    vorliegen.

19. Elektronischer Wahlrechner (Psephor, Urne) nach Anspruch 18, dadurch gekennzeichnet, daß dieser programmtechnisch so eingerichtet ist, daß auf er nur solche elektronischen Wahlscheine sammelt und/oder auswertet, die auch von einem elektronischen Wahlleiter signiert sind.

20. Elektronischer Wahlrechner (Psephor, Urne) nach Anspruch 16 oder 17, dadurch gekennzeichnet, daß der elektronische Wahlrechner die Auswertung in Form einer Zählung, vorzugsweise nach Wahlkategorien, der jeweils getroffenen Wahl vornimmt.

21. Elektronische Wahlstelle (Pollster), vorzugsweise ein Client-Rechner-System, welche, vorzugsweise über ein Telekommunikationsnetzwerk, mit einem elektronischen Wahlleiter (Validator), vorzugsweise einem ersten Server-Rechner-System und einem elektronischen Wahlrechner (Psephor, Urne), vorzugsweise einem zweiten Server-Rechner-System, verbunden ist, dadurch gekennzeichnet, daß sie programmtechnisch so eingerichtet ist, daß sie ihren Kommunikationsverkehr zum elektronischem Wahlleiter und zum elektronischen Wahlrechner nach dem Telekommunikationsprotokoll zur anonymen und authentischen Abwicklung einer elektronischen Wahl nach einem der Ansprüche 1 - 13 abwickelt.

22. Elektronische Wahlstelle (Pollster) nach Anspruch 21, dadurch gekennzeichnet, daß die elektronische Wahlstelle eine Lesevorrichtung zum Lesen eines elektronisch lesbaren Datenträgers, vorzugsweise eines nicht wiederbeschreibbaren Datenträgers, besonders bevorzugterweise einer Chipkarte (4) oder einer CD-ROM oder auch einer DVD, aufweist, die zur Authentifizierung oder Identifikation des Wählers mittels des nicht wiederbeschreibbaren Datenträgers dient.

23. Elektronische Wahlstelle (Pollster) nach Anspruch 21 oder 22, dadurch gekennzeichnet, daß die elektronische Wahlstelle eine Lesevorrichtung zur Durchführung einer biometrischen Identifikation, vorzugsweise einen Retina-Scanner oder ein Fingerabdrucklesegerät, besonders bevorzugterweise ein Sensorfeld (2), aufweist, die zur Identifikation des Wählers dient.

24. Elektronische Wahlstelle (Pollster) nach Anspruch 21, 22 oder 23, dadurch gekennzeichnet, daß die elektronische Wahlstelle ein elektronisches Stimmabgabe-Panel (1) aufweist.

25. Elektronische Wahlstelle (Pollster) nach einem der Ansprüche 21, 22, 23 oder 24, dadurch gekennzeichnet, daß die zum Betrieb der elektronischen Wahlstelle benötigten Software-Module auf nicht wiederbeschreibbarem Datenträger, vorzugsweise auf CD-ROM oder auf DVD vorliegen.

26. Computerprogrammprodukt mit Computerprogramm-Code-Mittel zum Laden in den Speicher eines Computers, wobei die Computerprogramm-Code-Mittel nach ihrem Laden einen Computer zum Betrieb des Telekommunikationsprotokolls nach einem der Ansprüche 1 bis 13 veranlassen, während das Computerprogramm auf dem Computer abläuft.

27. Computerprogramm auf einem elektronischen Trägersignal zum Laden in den Speicher eines Computers, welches nach Laden des Computerprogramms in den jeweiligen Computer diesen zum Betrieb des Telekommunikationsprotokolls nach einem der Ansprüche 1 bis 13 veranlaßt, während das Computerprogramm auf dem Computer abläuft.

FIG. 1

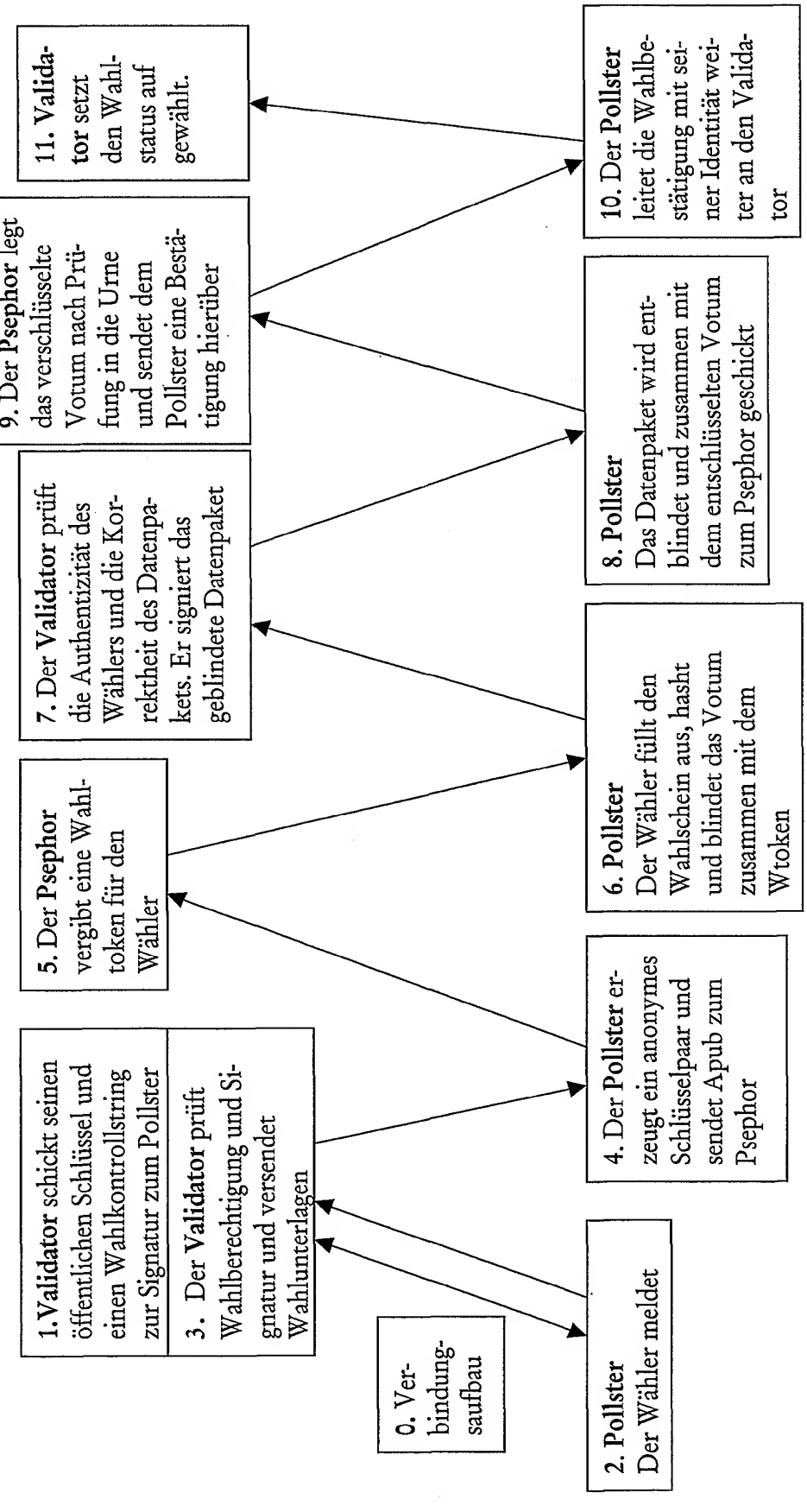

0. Verbindungsaufbau
1. Validator schickt seinen öffentlichen Schlüssel und einen Wahlkontrollstring zur Signatur zum Pollster
2. Pollster Der Wähler meldet
3. Der Validator prüft Wahlberechtigung und Signatur und versendet Wahlunterlagen
4. Der Pollster erzeugt ein anonymes Schlüsselpaar und sendet Apub zum Psephor
5. Der Psephor vergibt eine Wahltoken für den Wähler
6. Pollster Der Wähler füllt den Wahlschein aus, hasht und blindet das Votum zusammen mit dem Wtoken
7. Der Validator prüft die Authentizität des Wählers und die Korrektheit des Datenpakets. Er signiert das geblindete Datenpaket
8. Pollster Das Datenpaket wird entblindet und zusammen mit dem entschlüsselten Votum zum Psephor geschickt
9. Der Psephor legt das verschlüsselte Votum nach Prüfung in die Urne und sendet dem Pollster eine Bestätigung hierüber
10. Der Pollster leitet die Wahlbestätigung mit seiner Identität weiter an den Validator
11. Validator setzt den Wahlstatus auf gewählt.

Fig. 2

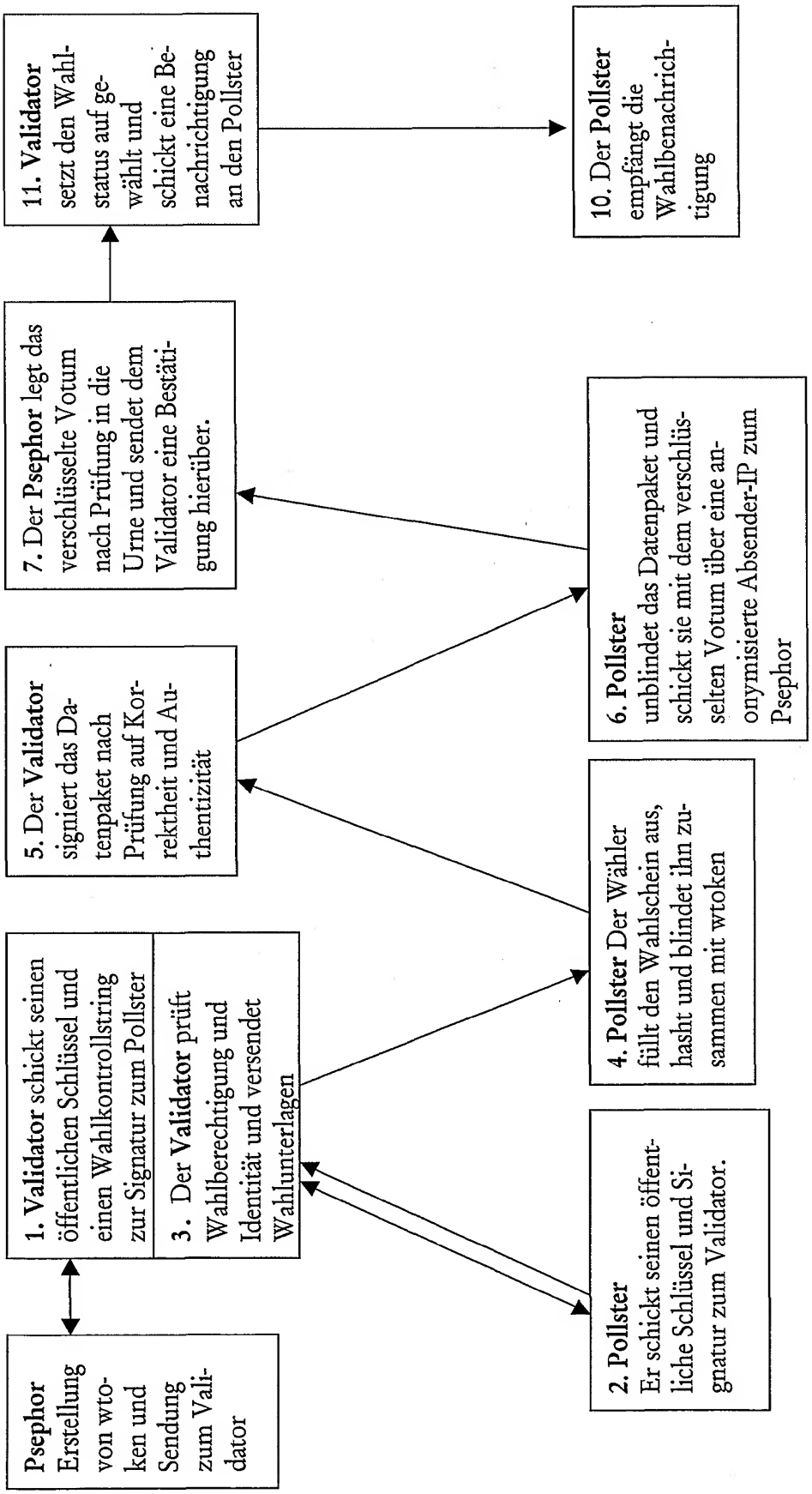

Psephor Erstellung von wtoken und Sendung zum Validator
1. Validator schickt seinen öffentlichen Schlüssel und einen Wahlkontrollstring zur Signatur zum Pollster
3. Der Validator prüft Wahlberechtigung und Identität und versendet Wahlunterlagen
2. Pollster Er schickt seinen öffentliche Schlüssel und Signatur zum Validator.
4. Pollster Der Wähler füllt den Wahlschein aus, hasht und blindet ihn zusammen mit wtoken
5. Der Validator signiert das Datenpaket nach Prüfung auf Korrektheit und Authentizität
6. Pollster unblindet das Datenpaket und schickt sie mit dem verschlüsselten Votum über eine anonymisierte Absender-IP zum Psephor
7. Der Psephor legt das verschlüsselte Votum nach Prüfung in die Urne und sendet dem Validator eine Bestätigung hierüber.
11. Validator setzt den Wahlstatus auf gewählt und schickt eine Benachrichtigung an den Pollster
10. Der Pollster empfängt die Wahlbenachrichtigung

FIG. 3

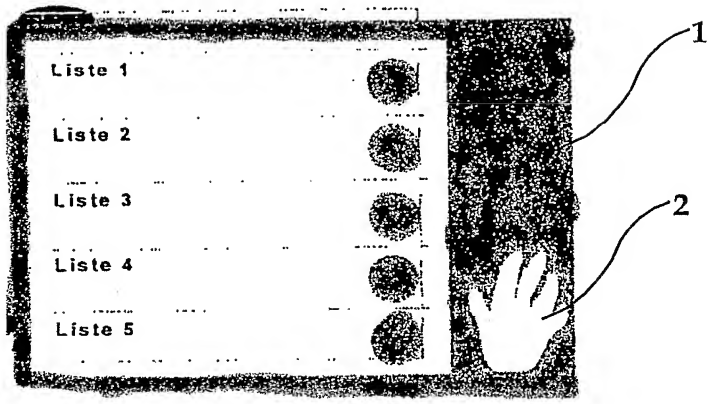


FIG. 4

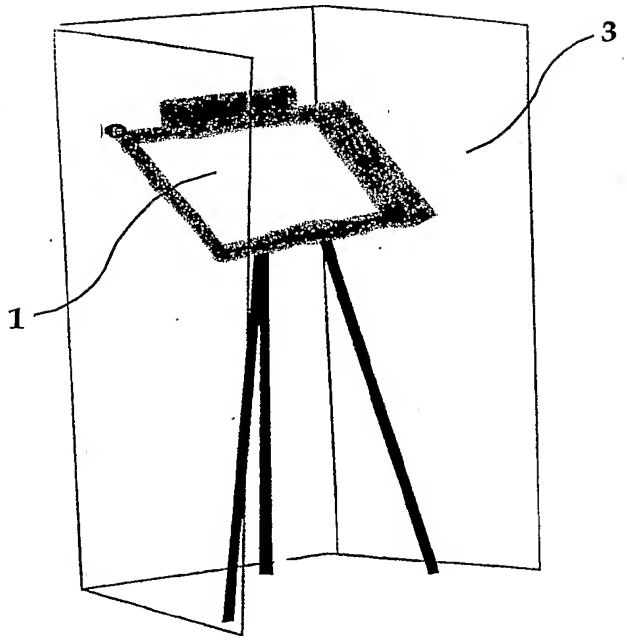
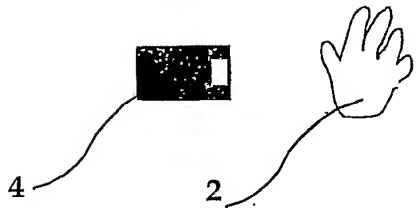


FIG. 5



INTERNATIONAL SEARCH REPORT

In nal Application No
F.,/DE 01/02334

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	BONETTI P ET AL: "The Italian academic community's electronic voting system" COMPUTER NETWORKS, ELSEVIER SCIENCE PUBLISHERS B.V., AMSTERDAM, NL, vol. 34, no. 6, December 2000 (2000-12), pages 851-860, XP004304824 ISSN: 1389-1286 abstract page 853, right-hand column, line 32 - line 37 page 854, left-hand column, line 42 -page 858, left-hand column, line 30 figure 2; table 1 --- -/--	1-7,9, 10, 12-22, 24-27

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 November 2001	20/11/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Masche, C

INTERNATIONAL SEARCH REPORT

Int ›nal Application No
PC[illegible]/DE 01/02334

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	CRANOR L F ET AL: "SENSUS: A SECURITY-CONSCIOUS ELECTRONIC POLLING SYSTEM FOR THE INTERNET" PROCEEDINGS OF THE HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES, XX, XX, vol. 3, 7 January 1997 (1997-01-07), pages 561-570, XP002929749 page 563, right-hand column, line 20 - line 38 page 564, left-hand column, line 18 -page 566, left-hand column, line 5 figure 1 ---	1-6, 9-12, 14-21, 26,27
X	MU Y ET AL: "ANONYMOUS SECURE E-VOTING OVER A NETWORK" PROCEEDINGS. ANNUAL COMPUTER SECURITY APPLICATIONS CONFERENCE, XX, XX, vol. 14, CONF, 1998, pages 293-299, XP000869577 page 295, right-hand column, line 1 -page 297, left-hand column, line 41 page 298, left-hand column, line 8 - line 22 ---	1-7, 9-12, 14-21, 26,27
X	US 6 081 793 A (CHALLENER DAVID C ET AL) 27 June 2000 (2000-06-27) abstract column 9, line 28 -column 10, line 50 figures 9A-D -----	1-3,5,6, 9,14-22, 26,27

INTERNATIONAL SEARCH REPORT

formation on patent family members

In ınal Application No
PCT/DE 01/02334

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6081793 A	27-06-2000	NONE	

INTERNATIONALER RECHERCHENBERICHT

In nales Aktenzeichen
PCT/DE 01/02334

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04L9/32

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, INSPEC

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	BONETTI P ET AL: "The Italian academic community's electronic voting system" COMPUTER NETWORKS, ELSEVIER SCIENCE PUBLISHERS B.V., AMSTERDAM, NL, Bd. 34, Nr. 6, Dezember 2000 (2000-12), Seiten 851-860, XP004304824 ISSN: 1389-1286 Zusammenfassung Seite 853, rechte Spalte, Zeile 32 - Zeile 37 Seite 854, linke Spalte, Zeile 42 -Seite 858, linke Spalte, Zeile 30 Abbildung 2; Tabelle 1 --- -/--	1-7,9, 10, 12-22, 24-27

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
12. November 2001	20/11/2001

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Masche, C

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	CRANOR L F ET AL: "SENSUS: A SECURITY-CONSCIOUS ELECTRONIC POLLING SYSTEM FOR THE INTERNET" PROCEEDINGS OF THE HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES, XX, XX, Bd. 3, 7. Januar 1997 (1997-01-07), Seiten 561-570, XP002929749 Seite 563, rechte Spalte, Zeile 20 - Zeile 38 Seite 564, linke Spalte, Zeile 18 -Seite 566, linke Spalte, Zeile 5 Abbildung 1 ---	1-6, 9-12, 14-21, 26,27
X	MU Y ET AL: "ANONYMOUS SECURE E-VOTING OVER A NETWORK" PROCEEDINGS. ANNUAL COMPUTER SECURITY APPLICATIONS CONFERENCE, XX, XX, Bd. 14, CONF, 1998, Seiten 293-299, XP000869577 Seite 295, rechte Spalte, Zeile 1 -Seite 297, linke Spalte, Zeile 41 Seite 298, linke Spalte, Zeile 8 - Zeile 22 ---	1-7, 9-12, 14-21, 26,27
X	US 6 081 793 A (CHALLENER DAVID C ET AL) 27. Juni 2000 (2000-06-27) Zusammenfassung Spalte 9, Zeile 28 -Spalte 10, Zeile 50 Abbildungen 9A-D -----	1-3,5,6, 9,14-22, 26,27

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlich die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/DE 01/02334

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 6081793 A	27-06-2000	KEINE	